

Student Affairs Device Management Standard

1. Purpose

This standard establishes guidelines for the lifecycle management of all devices within Student Affairs, ensuring consistent practices for device authorization, purchase, setup, deployment, management, updates, disposal, and asset tracking.

2. Scope

This standard applies to all departments within the Student Affairs organization and covers all electronic devices used for official purposes, including but not limited to computers, laptops, tablets, and smartphones.

3. Device Lifecycle Management

3.1 Authorization and Purchase

- All computing hardware purchases, such as workstations, laptops, and mobile devices, must receive prior authorization from the IT department.
- Departments will submit a purchase request form specifying device requirements and intended use. (The purchase request form is in the final stages and will be available in January.)
- The Student Affairs IT department will review each request to ensure compatibility with current systems and adherence to security standards.
- All computing devices must be procured from authorized vendors or suppliers as specified by the procurement department.

3.2 Device Setup

- All new computing devices will be set up by the IT department, which includes:
 - Imaging the device with the institution-approved operating system
 - Installing approved software packages
 - Setting up device management agents.

- Configuring initial security settings
- Configuring network settings

3.3 Deployment

- The IT department is responsible for deploying all devices to end-users or departments. During deployment, IT will:
 - Verify device functionality
 - Provide basic user training if necessary
 - Document, device information (serial number, asset tag, assigned user/department)

3.4 Device Management

- All devices will be managed using one of the following platforms:
 - Kaseya
 - JAMF
 - BigFix
- Splunk will be integrated for audit log backups.
- Microsoft Defender will be installed on all devices for virus protection and monitoring.
- All devices must be joined to the DSA domain.
- Group Policy rules will be applied to enhance security and ensure consistent configuration.

3.5 Updates and Patches

- Regular updates and security patches will be applied through designated management tools.
- Users and departments are responsible for:
 - Ensuring devices remain physically secure
 - Keeping devices powered on and connected to the network regularly to receive updates
 - Promptly restarting devices when required for updates
 - Ensuring that any user with multiple IT assets connects them to the network at least once a month for a 24-hour cycle to allow management applications to update device information. Users should check for updates manually when able.

- Departments with laptops that are not regularly used must power on devices and connect them to the network for a 24-hour cycle and check for updates manually during that period.

3.6 Device Disposal

- Departments must coordinate with the IT department when a device is no longer needed or has reached end-of-life by submitting a device surplus request through [ServiceNow](#).
- IT will ensure all data is securely erased from the device before disposal.
- Devices must be sent to surplus following institutional procedures.
- IT will maintain records of all disposed devices.

Steps to Properly Remove a Computer Asset from Student Affairs Inventory:

1. Complete the IT Support Request to surplus computing hardware.
2. SAIT will pick up the device.
3. Depending on the device, the following will be completed:
 - **For laptops and PCs:** SAIT will remove the hard drive.
 - **For tablets or Apple products:** SAIT will wipe computing data and reset the device to factory default.
4. SAIT will remove the device from the domain and the management system.
5. SAIT will close the IT Support Request ticket.
6. SAIT will process surplus requests and schedule hardware pickup
7. Enter device details into the VT Surplus website by SAIT.
8. Obtain approval for surplus items.
9. VT Surplus will pick up the device.

Notes:

- Hard drives are sent to Surplus by SAIT for a records destruction process.
- All non-computing hardware surplus requests should be submitted by the asset coordinator (e.g., monitors, keyboards, mice, printers, and other computer peripherals).

3.7 Fixed Asset Management

- Each department must designate a Fixed Asset Coordinator.
- Fixed Asset Coordinators are responsible for:
 - Maintaining accurate records of all devices assigned to their department
 - Updating device location and custodian information as changes occur
 - Conducting regular inventory checks (at least annually)
 - Reporting any discrepancies to the IT department immediately

4. Compliance

- All departments and users are required to adhere to this Device Management Standard, as well as all other university standards pertaining to device usage.
- Failure to comply may result in the disabling of the device or its isolation from the Virginia Tech network.

5. Review and Updates

- This standard will be reviewed annually by the IT department and updated as necessary to reflect changes in technology, security requirements, or organizational needs.
- Any proposed changes to this standard must be approved by the IT Director and communicated to all departments.

6. Contact Information

For questions or assistance regarding this standard, please contact:
dsaitsupport@vt.edu